

Security Principles: Defenses

SPR500 NBB

Project

Security Testing Report

Group 2	
Student Name	Student ID
Khondoker Ishmum Muhammad	155895212
Yash Siraj Devani	160409215
Ananthu Krishna Vadakkeppatt	154290217
Aryan Santosh Saindane	136235215

Table Of Contents

Table Of Contents.....	2
Executive Summary.....	3
Recommended Controls & Controls Tested.....	4
1. SQL Injection Prevention.....	4
2. Vulnerability Scanning.....	5
3. Proactive Monitoring.....	5
4. Network Segmentation Validation.....	6
5. Continuous DNS Monitoring.....	7
6. Web Application Security.....	8
7. DNS Security.....	9
8. File Inclusion Prevention.....	10
9. SQL Injection Blind.....	11
10. Company asset (hardware & software) management.....	11
11. Malware Defense Control.....	12
12. Incident Response Planning.....	13
13. Regular Security Assessments for Active Directory.....	13
14. Lateral Movement Prevention.....	14
15. Account Access Management.....	15
16. SSL Certificates & CA For Secure HTTPS and Trust In Browser.....	15
17. Host based Firewall utilization.....	17
18. Active Directory Domain User & Groups Management.....	18
Conclusion.....	19

Executive Summary

The objective of this report is to highlight the testing of security controls implemented in the Agricore infrastructure. Recognizing the pivotal role of security controls in protecting digital assets and sensitive information within the domain, the report emphasizes the proactive identification and mitigation of vulnerabilities and weaknesses. Utilizing security control testing serves as a strategic approach to fortify defenses against potential threats, ensuring the integrity of networks, and instilling confidence with clients. The security controls, implemented in accordance with the CIS framework, are central to this discussion. The report aims to elucidate the process of adding and testing these controls within the Agricore infrastructure.

Recommended Controls & Controls Tested Based On CIS

Below we showcase 18 security controls that are based on the CIS controls. These controls will help ensure proper security posture for the organizations and allow smooth business operations.

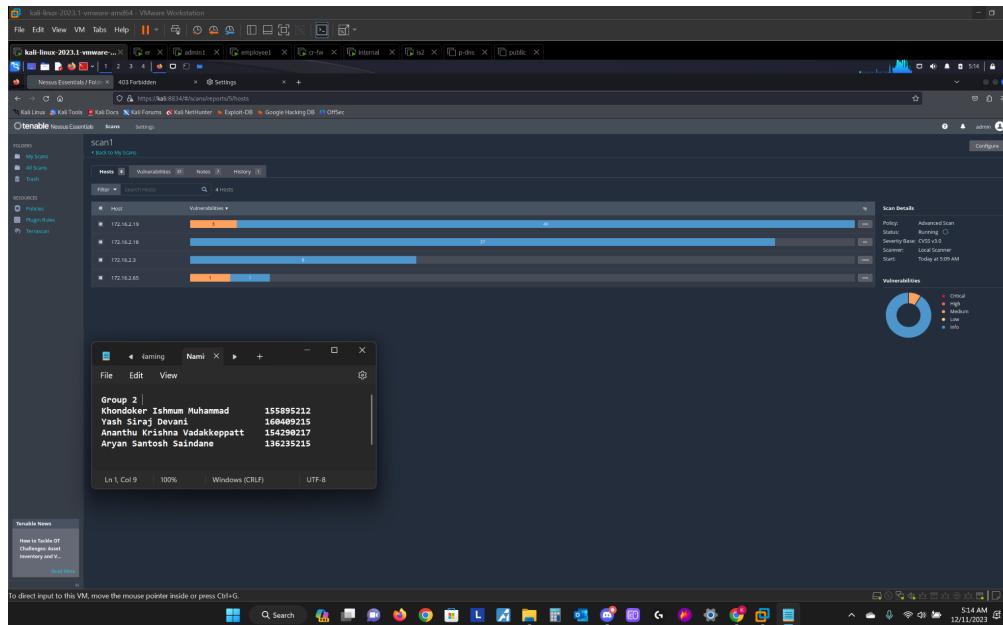
1. SQL Injection Prevention

- Implementing a Web Application Firewall (WAF) is crucial for enhancing the security posture of your web applications. SQL Injection blocked and logged.



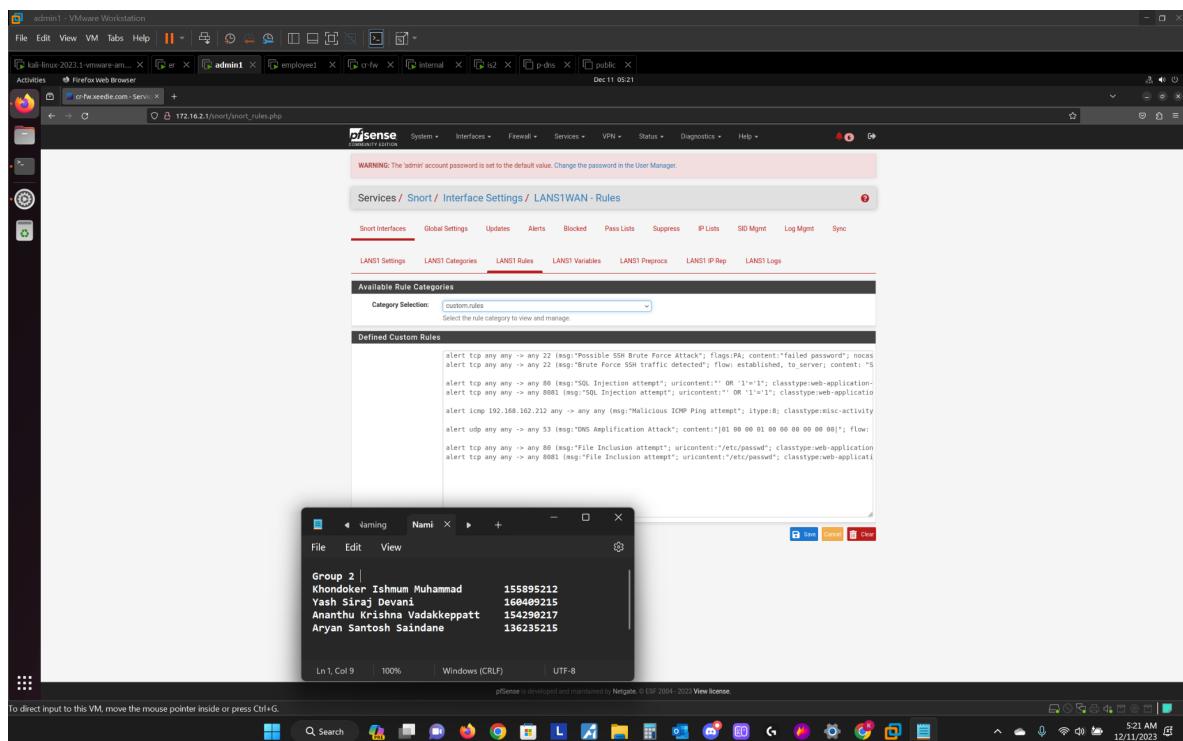
2. Vulnerability Scanning

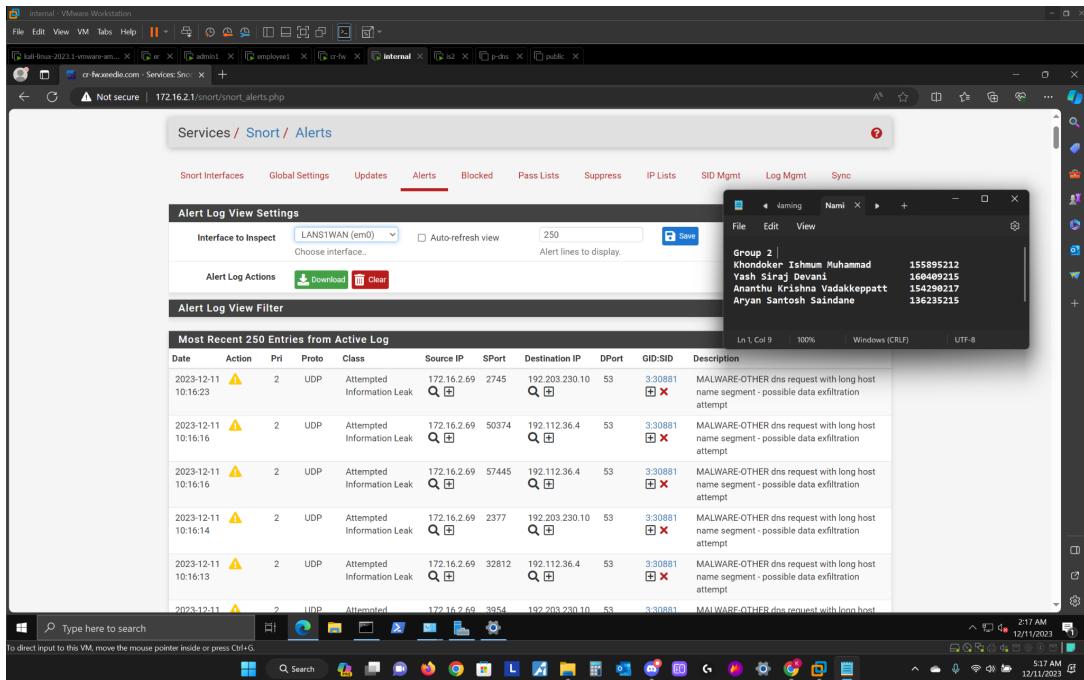
- Utilize automated vulnerability scanning tools to identify and prioritize patching for critical vulnerabilities. Utilize nessus for scanning or nmap.



3. Proactive Monitoring

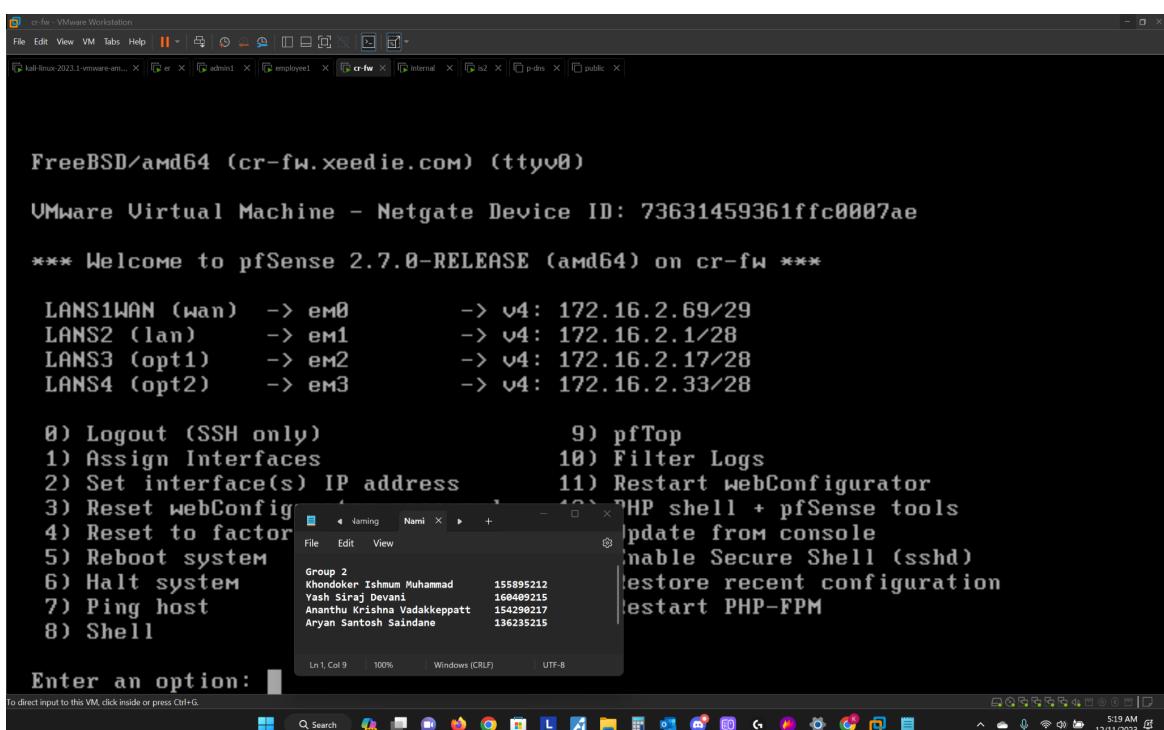
- Emphasize the importance of proactive monitoring for early detection of security incidents. Utilize Snort IDS to monitor traffic. Also utilize custom snort rules.

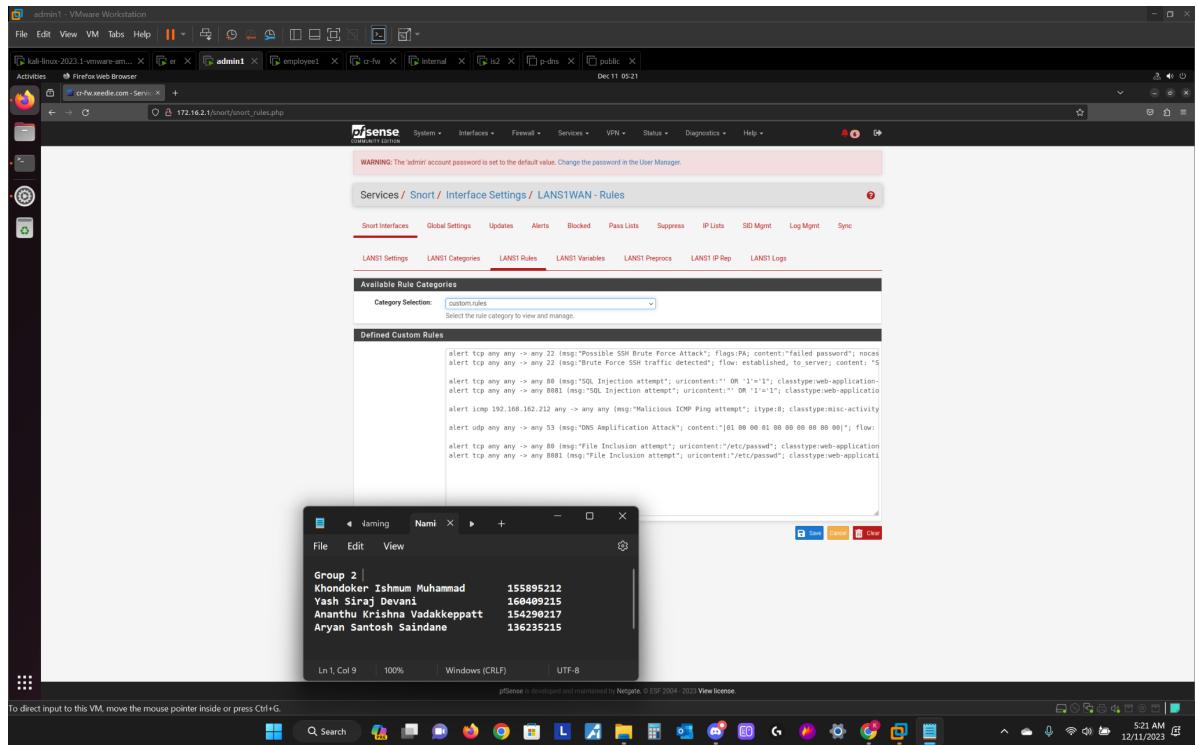




4. Network Segmentation Validation

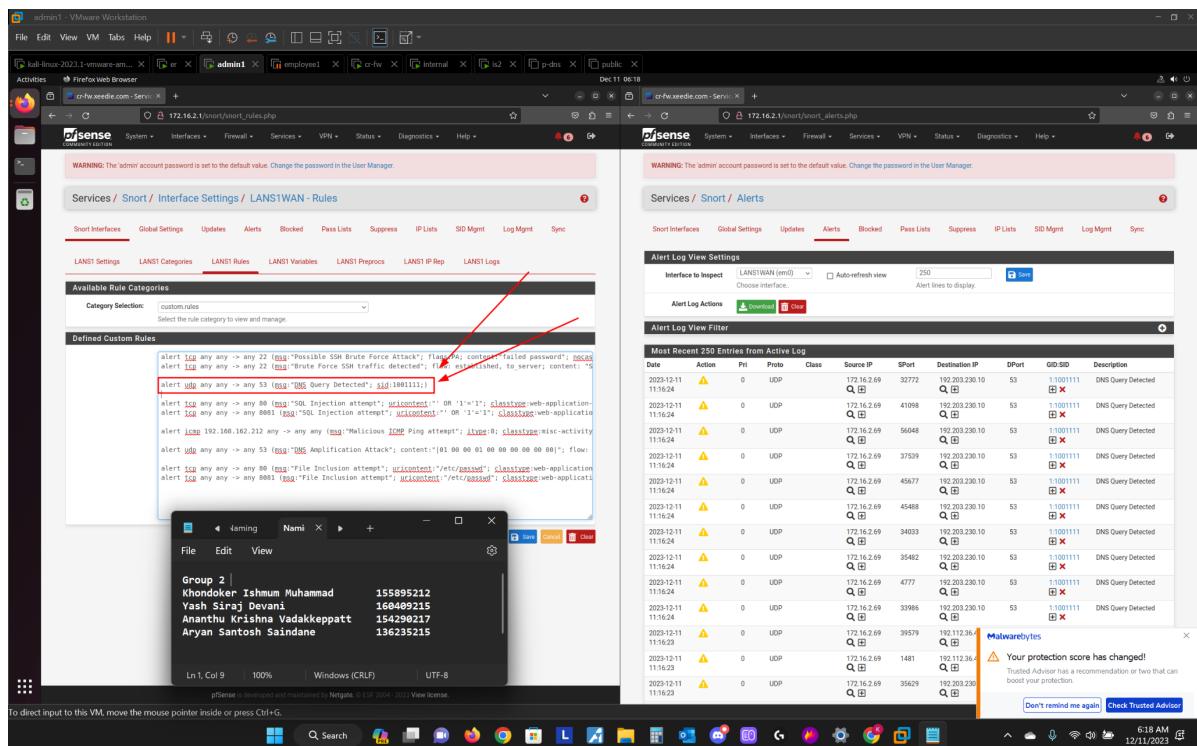
- Include a recommendation to conduct regular penetration testing to validate the effectiveness of network segmentation controls. Creating different LANs for different parts of our networks.





5. Continuous DNS Monitoring

- Emphasize the importance of continuous monitoring and timely response to DNS-related security events. Snort IDS can be used here.



6. Web Application Security

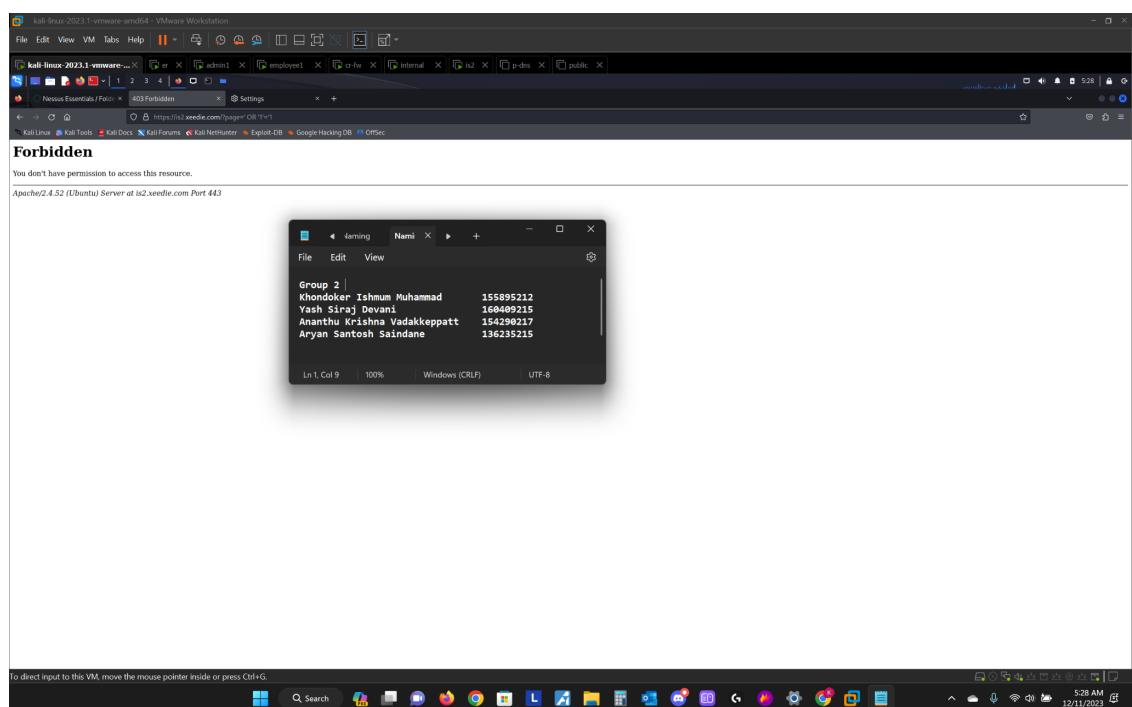
- Implementing Web Applications Firewall (WAFs) to monitor and filter HTTP traffic, enhancing protection against input validation vulnerabilities. Utilize Mod Security. Below we can see mod security blocking and logging the sql injection attack.

The screenshot shows a terminal window on a Kali Linux VM. The user has run the command `ls -l /usr/share/modsecurity-crs/rules` to list the contents of the ModSecurity rules directory. The output shows numerous files related to various security rules, such as `iis-errors.data`, `java-classes.data`, and `php-config-directives.data`. The user has also run `cat /etc/apache2/sites-available/000-default.conf` to view the Apache configuration file, which includes the ModSecurity module configuration. A second terminal window shows the Apache error log with several entries indicating requests blocked by ModSecurity, such as REQUEST-900-EXCLUSION-RULES-BEFORE-CRASH and REQUEST-901-INITIALIZATION_CONF.

```

spr500@ls2:~$ ls -l /usr/share/modsecurity-crs/rules
total 852
drwxr-xr-x 2 root root 4096 Nov 22 11:22 .
drwxr-xr-x 10 root root 4096 Nov 22 11:22 ..
-rw-r--r-- 1 root root 4215 Nov 22 11:22 iis-errors.data
-rw-r--r-- 1 root root 1826 Nov 22 11:22 java-classes.data
-rw-r--r-- 1 root root 264 Nov 22 11:22 java-code-leakages.data
-rw-r--r-- 1 root root 240 Nov 22 11:22 java-errors.data
-rw-r--r-- 1 root root 12765 Nov 22 11:22 php-config-directives.data
-rw-r--r-- 1 root root 75823 Nov 22 11:22 php-errors.data
-rw-r--r-- 1 root root 139 Nov 22 11:22 php-errors-p12.data
-rw-r--r-- 1 root root 3414 Nov 22 11:22 php-function-names-933150.data
-rw-r--r-- 1 root root 38099 Nov 22 11:22 php-function-names-933151.data
-rw-r--r-- 1 root root 610 Nov 22 11:22 php-variables.data
-rw-r--r-- 1 root root 9055 Nov 22 11:22 REQUEST-900-EXCLUSION-RULES-BEFORE-CRASH
-rw-r--r-- 1 root root 13861 Nov 22 11:22 REQUEST-901-INITIALIZATION_CONF
-rw-r--r-- 1 root root 1659 Nov 22 11:22 REQUEST-905-COMMON-EXCEPTIONS_CONF
-rw-r--r-- 1 root root 2700 Nov 22 11:22 REQUEST-911-METHOD-ENFORCEMENT_CONF
-rw-r--r-- 1 root root 3340 Nov 22 11:22 REQUEST-913-SCANNER-DETECTION_CONF
-rw-r--r-- 1 root root 62234 Nov 22 11:22 REQUEST-928-PROTOCOL-ENFORCEMENT_CONF
f
-rw-r--r-- 1 root root 20803 Nov 22 11:22 REQUEST-921-PROTOCOL-ATTACK_CONF
-rw-r--r-- 1 root root 4576 Nov 22 11:22 REQUEST-922-MULTIPART-ATTACK_CONF
-rw-r--r-- 1 root root 7857 Nov 22 11:22 REQUEST-930-APPLICATION-ATTACK-LFI_CONF
onf
-rw-r--r-- 1 root root 8650 Nov 22 11:22 REQUEST-931-APPLICATION-ATTACK-RFI_CONF
onf
-rw-r--r-- 1 root root 134885 Nov 22 11:22 REQUEST-932-APPLICATION-ATTACK-RCE_CONF
onf
-rw-r--r-- 1 root root 32185 Nov 22 11:22 REQUEST-933-APPLICATION-ATTACK-PHP_CONF
onf
-rw-r--r-- 1 root root 28281 Nov 22 11:22 REQUEST-934-APPLICATION-ATTACK-GENERAL_CONF

spr500@ls2:~$ cat /etc/apache2/sites-available/000-default.conf
</VirtualHost>
spr500@ls2:~$ cat /etc/apache2/sites-available/000-default.conf
<VirtualHost 172.16.2.19:443>
    ServerName ts2.xeedte.com
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html
    SSLEngine on
    SSLCertificateFile "/home/spr500/icerts/ls2.xeedte.com.crt"
    SSLCertificateKeyFile "/home/spr500/icerts/ls2.xeedte.com.key"
    SSLCACertificateFile "/home/spr500/icerts/miICA.pem"
    SecRuleEngine On
    <IfModule _modsec2_.module>
        Include /usr/share/modsecurity-crs/crs-setup.conf
        Include /usr/share/modsecurity-crs/rules/*.conf
    </IfModule>
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
spr500@ls2:~$ 
```



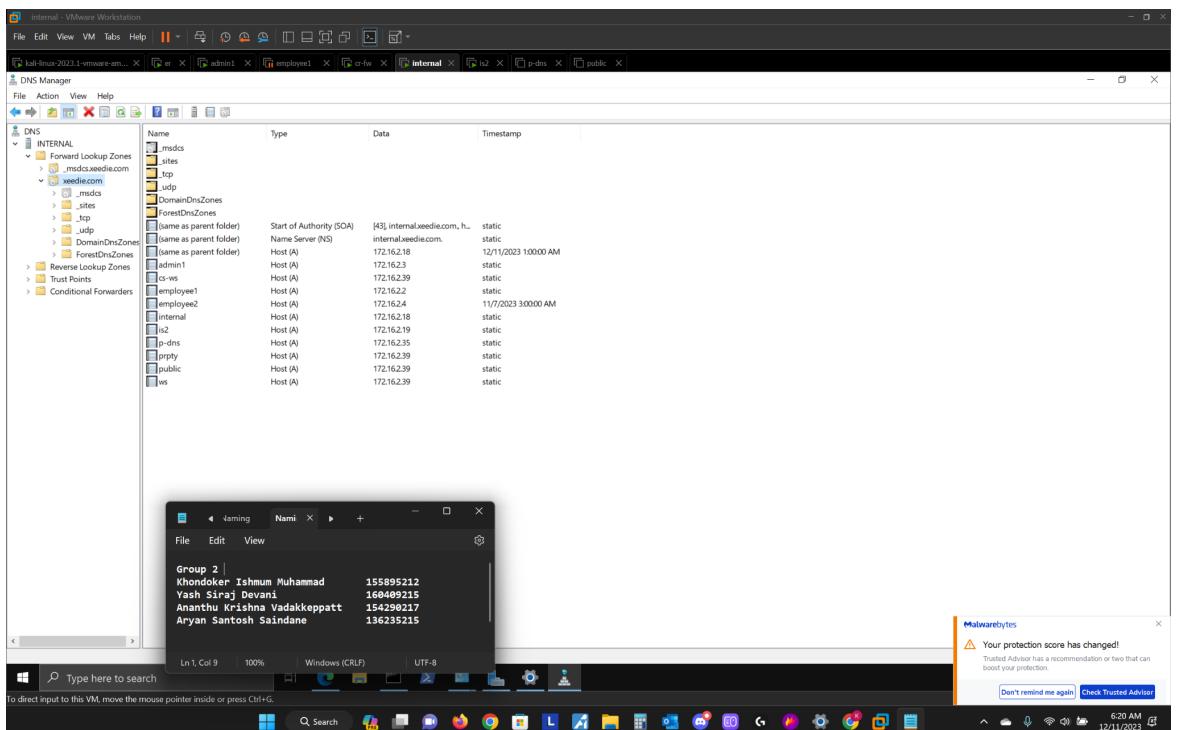
```
File Edit View VM Tabs Help || Activities Terminal Dec 11 05:27
[full-linux-2023.1.vmware-smu... X er X admin X employed X cr-fw X internal X ls2 X p-dns X public X
sp@5000:~/.ver/log/apache2

emote Command Execution: Unix Shell Code Found" [data "Matched Data: dev/tcp found within ARG$:/name[]: $(bash -c echo exploited_port[443]by_nessus>/dev/tcp[172.16.2.5/32777]" [severity "CRITICAL"] [ver "OWASP CRS/4.0.0-rc2"] [tag "application-multi"] [tag "language-shell"] [tag "platform-unix"] [tag "attack-rce"] [tag "paranoia-level/1"] [ver "OWASP CRS"] [tag "capec/1000/152/248/88"] [tag "PCI/6.5.2"] [hostname "ls2.xeedie.com"] [uri "/api/getServices"] [unique_id "ZXbzqzLAYtAD7GUajk7XVzwAAEo"]
[Mon Dec 11 05:13:34.284143 2023] [security:error] [pid 1141:tid 140362936964672] [client 172.16.2.5:40792] [client 172.16.2.5] ModSecurity: Access denied with code 403 (phase 2). Operator GE matched 5 at TX:blocking_inbound_anomaly_score. [file "/usr/share/modsecurity-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "186"] [id "94910"] [msg "Inbound Anomaly Score Exceeded (Total Score: 15)" [ver "OWASP CRS/4.0.0-rc2"] [tag "anomaly-evaluation"] [hostname "ls2.xeedie.com"] [uri "/api/getServices"] [unique_id "ZXbzqzLAYtAD7GUajk7XVzwAAEo"]
[Mon Dec 11 05:13:34.284669 2023] [conditional match in SecAction. [file bound Scores: blocking=15, detection=0, per_pl=0-0-0-0, threshold=4 - (SQLI=0 XSS=0, RFI=0, LFI=0, RCE=15, PHPINFO=0, " /api/getServices"] [unique_id "ZXbzqzLAYtAD7GUajk7XVzwAAEo"]
Group 2
Khondoker Ishummuhammad 155895212
Yash Siraj Devani 160409519
Ananthu Krishna Vadakkepatt 154296217
Aryan Santosh Saindane 136235215
[Mon Dec 11 05:13:37.061163 2023] [rator EQ matched 0 at REQUEST_HEADERS Containing Content, but Missed quest ] [tag "platform-multi"] [tag "attack-rce"] [functionRouter] [unique_id "ZXbzqzLAYtAD7GUajk7XVzwAAEo"]
[Mon Dec 11 05:13:37.061251 2023] [conditional match in SecAction. [file bound Scores: blocking=2, detection=2, per_pl=2-0-0-0, threshold=5 - (Outbound Scores: blocking=0, detection=0, per_pl=0-0-0-0, threshold=4) . (SQLI=0, XSS=0, RFI=0, LFI=0, RCE=0, PHPINFO=0, HTTP=0, SESS=0, COMBINED_SCORE=2)] [ver "OWASP CRS/4.0.0-rc2"] [tag "reporting"] [hostname "ls2.xeedie.com"] [uri "/functionRouter"] [unique_id "ZXbzqzLAYtAD7GUajk7XVzwAAFy"]
[Mon Dec 11 05:27:20.053013 2023] [security:error] [pid 1141:tid 140362962142784] [client 172.16.2.5:57760] [client 172.16.2.5] ModSecurity: Warning. detected SQLi using libinjection with fingerprints &sos& [file "/usr/share/modsecurity-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "66"] [id "942100"] [msg "SQL Injection Attack Detected via libinjection"] [data "Matched Data: &sos found within ARG$:/page: ' OR '1='1'" [severity "CRITICAL"] [ver "OWASP CRS/4.0.0-rc2"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-sql"] [tag "paranoia-level/1"] [tag "OWASP CRS"] [tag "capec/1000/152/248/66"] [tag "PCI/6.5.2"] [hostname "ls2.xeedie.com"] [uri "/"] [unique_id "ZxbkCFAYtAD7GUajk7XVzwAAEo"]
[Mon Dec 11 05:27:20.053478 2023] [security:error] [pid 1141:tid 140362962142784] [client 172.16.2.5:57760] [client 172.16.2.5] ModSecurity: Access denied with code 403 (phase 2). Operator GE matched 5 at TX:blocking_inbound_anomaly_score. [file "/usr/share/modsecurity-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "186"] [id "94910"] [msg "Inbound Anomaly Score Exceeded (Total Score: 5)" [ver "OWASP CRS/4.0.0-rc2"] [tag "anomaly-evaluation"] [hostname "ls2.xeedie.com"] [uri "/"] [unique_id "ZxbkCFAYtAD7GUajk7XVzwAAEo"]
[Mon Dec 11 05:27:20.053582 2023] [security:error] [pid 1141:tid 140362962142784] [client 172.16.2.5:57760] [client 172.16.2.5] ModSecurity: Warning. Unc conditional match in SecAction. [file "/usr/share/modsecurity-crs/rules/RESPONSE-980-CORRELATION.conf"] [line "96"] [id "980170"] [msg "Anomaly Scores: (Inbound Scores: blocking=5, detection=5, per_pl=5-0-0-0, threshold=5) (Outbound Scores: blocking=0, detection=0, per_pl=0-0-0-0, threshold=4) . (SQLI=5, XSS=0, RFI=0, LFI=0, RCE=0, PHPINFO=0, HTTP=0, SESS=0, COMBINED_SCORE=5)] [ver "OWASP CRS/4.0.0-rc2"] [tag "reporting"] [hostname "ls2.xeedie.com"] [uri "/"] [unique_id "ZxbkCFAYtAD7GUajk7XVzwAAEo"]
[Mon Dec 11 05:27:20.053582 2023] [security:error] [pid 1141:tid 140362962142784] [client 172.16.2.5:57760] [client 172.16.2.5] ModSecurity: Warning. Unc conditional match in SecAction. [file "/usr/share/modsecurity-crs/rules/RESPONSE-980-CORRELATION.conf"] [line "96"] [id "980170"] [msg "Anomaly Scores: (Inbound Scores: blocking=5, detection=5, per_pl=5-0-0-0, threshold=5) (Outbound Scores: blocking=0, detection=0, per_pl=0-0-0-0, threshold=4) . (SQLI=5, XSS=0, RFI=0, LFI=0, RCE=0, PHPINFO=0, HTTP=0, SESS=0, COMBINED_SCORE=5)] [ver "OWASP CRS/4.0.0-rc2"] [tag "reporting"] [hostname "ls2.xeedie.com"] [uri "/"] [unique_id "ZxbkCFAYtAD7GUajk7XVzwAAEo"]

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

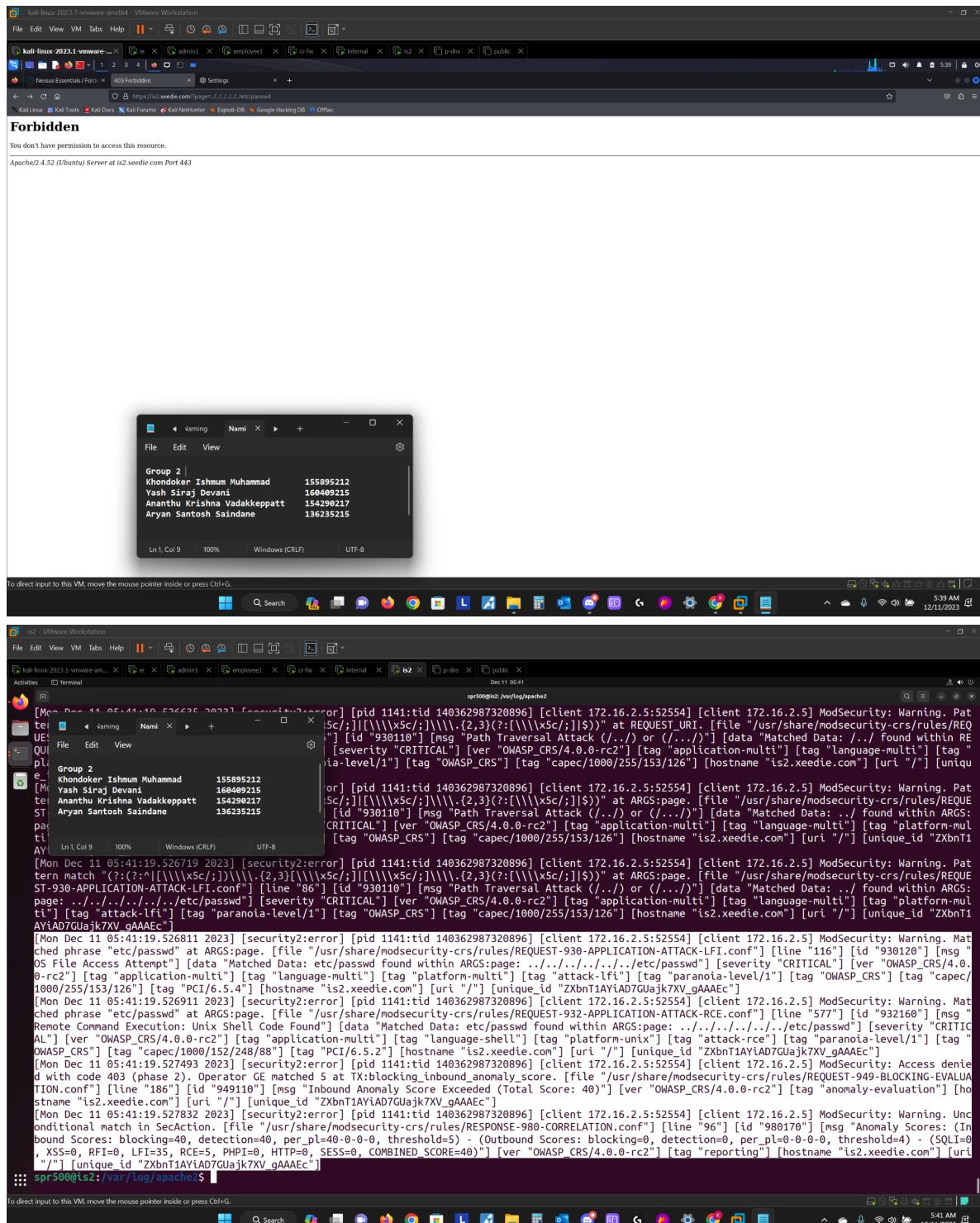
7. DNS Security

- Regularly review and update DNS configurations to ensure the integrity and security of DNS services.



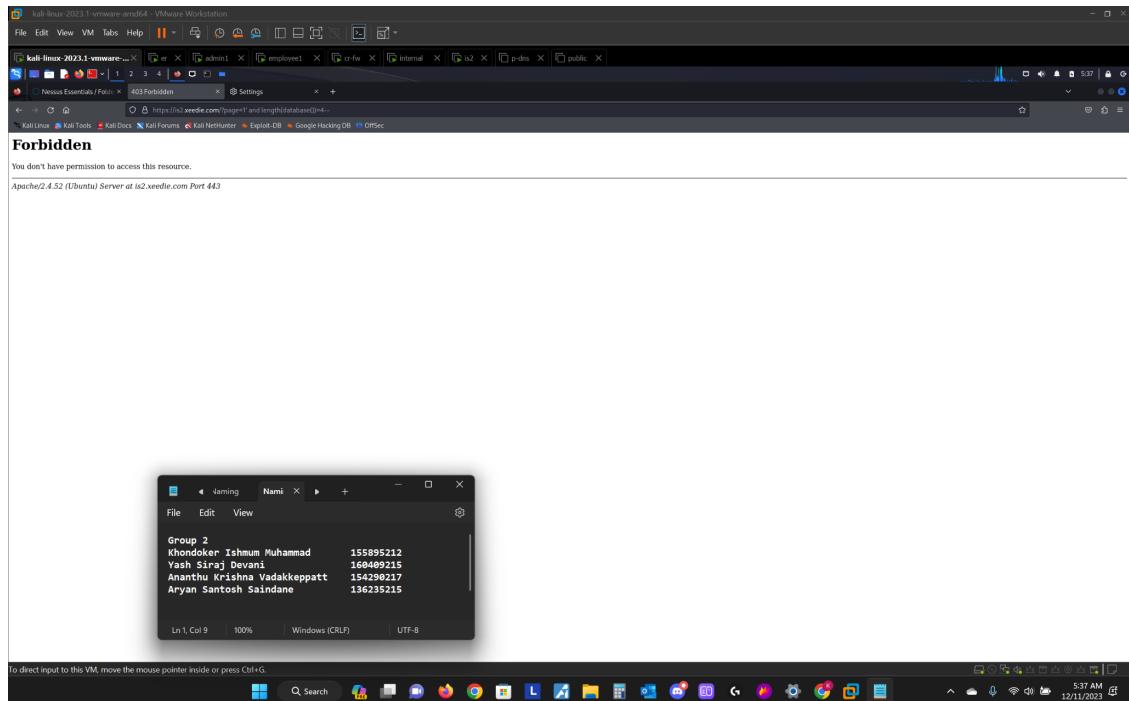
8. File Inclusion Prevention

- Deploy a WAF to monitor and filter HTTP traffic, providing an additional layer of defense against file inclusion vulnerabilities. File inclusions attack blocked and logged.



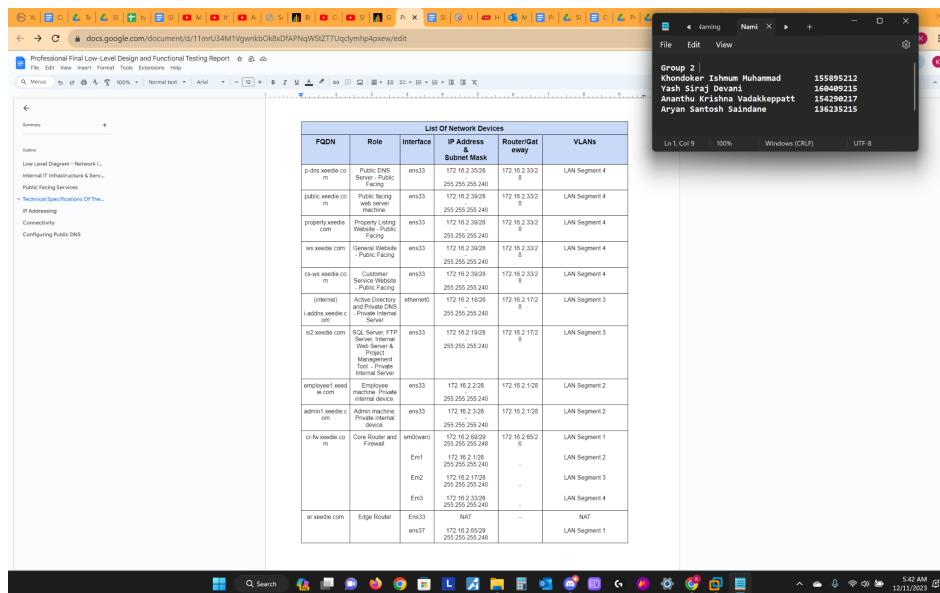
9. SQL Injection Blind

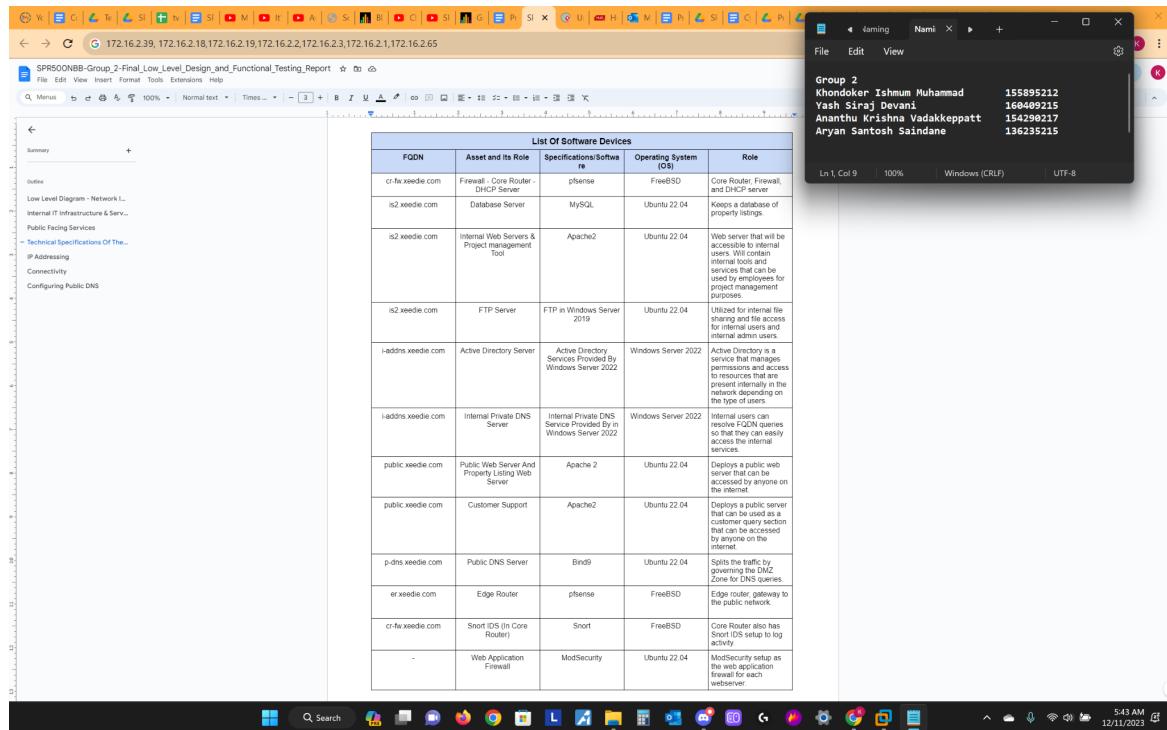
- Deploy a WAF to actively monitor and filter HTTP traffic, providing an effective defense against Blind SQL Injection attempts.



10. Company asset (hardware & software) management

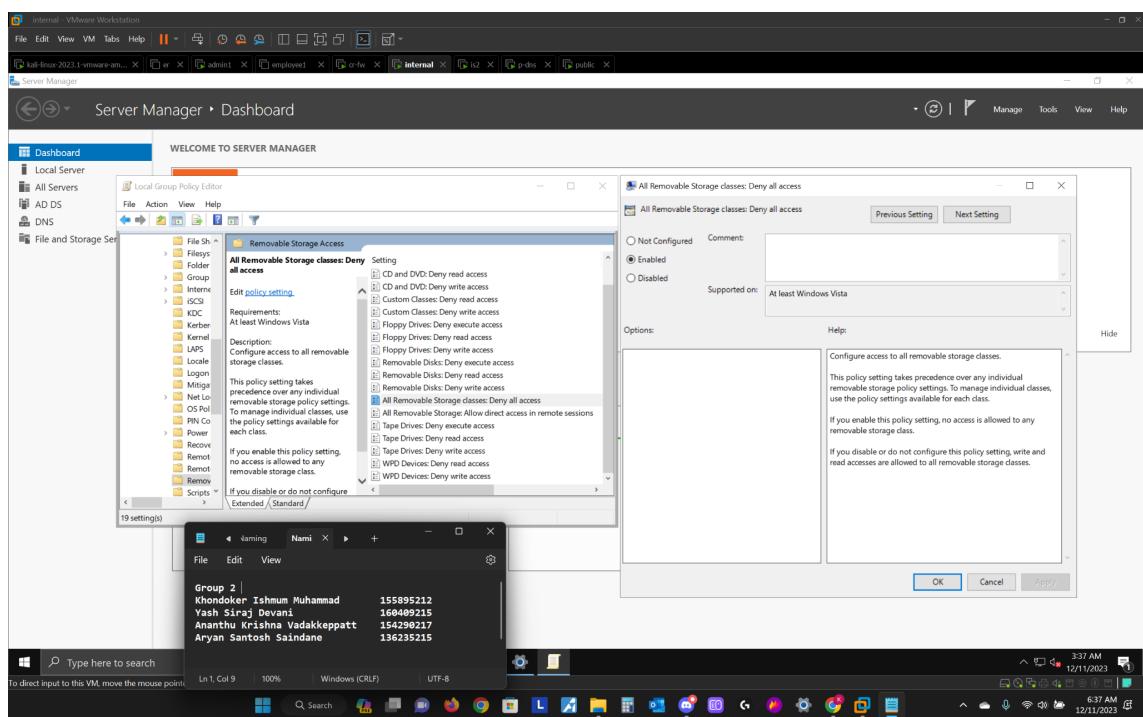
- Crucial for compliance and cost optimization, involves tracking software assets, including installed applications, across the organization's end-user devices, servers, and virtual environments.

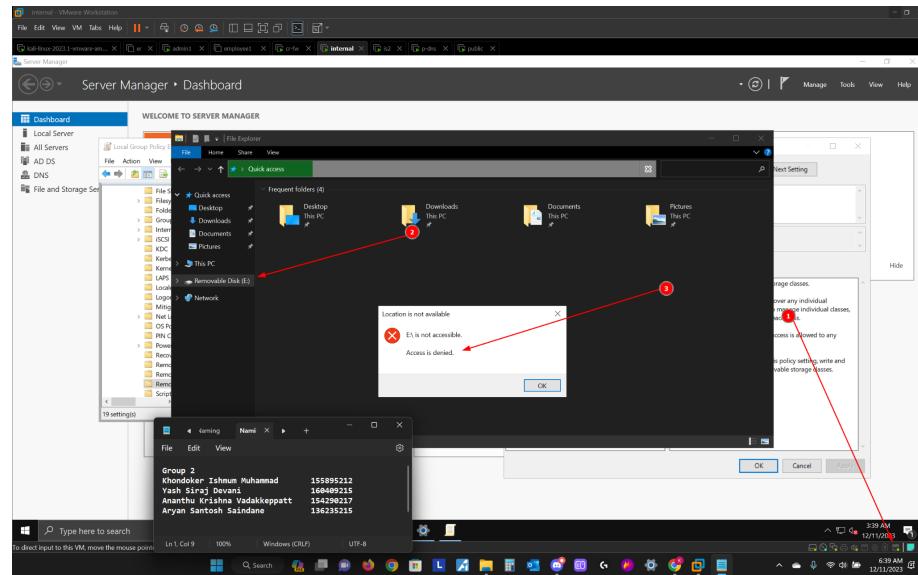




11. Malware Defense Control

- Implementing critical malware defense measures, we disabled autorun on all connected devices through a Group Policy Object (GPO), preventing the automatic execution of malware on USB drive connection, and extended this control to Proxmox infrastructure, prohibiting the attachment of removable devices for enhanced security.



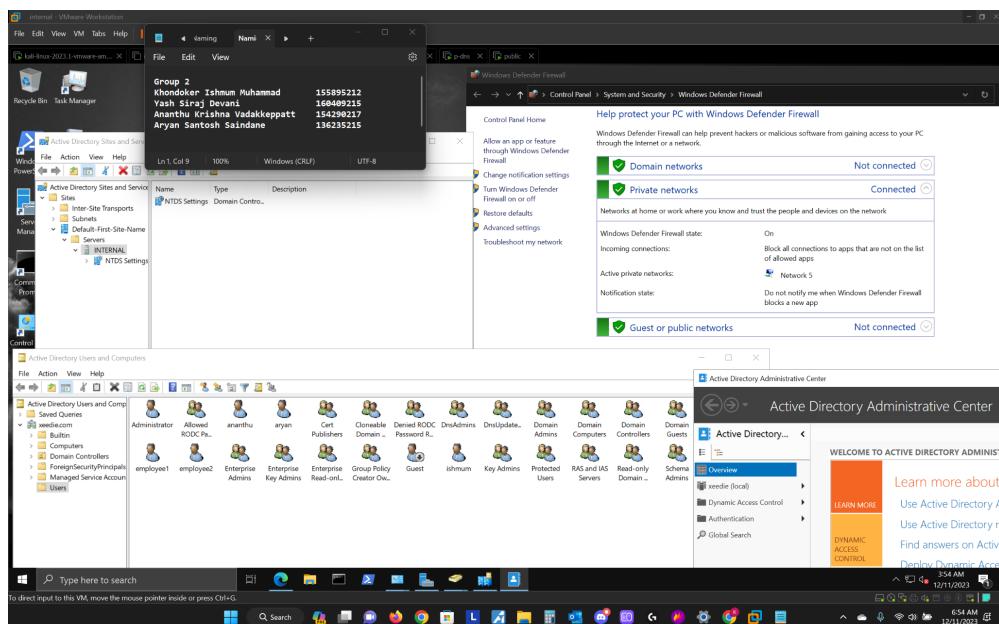


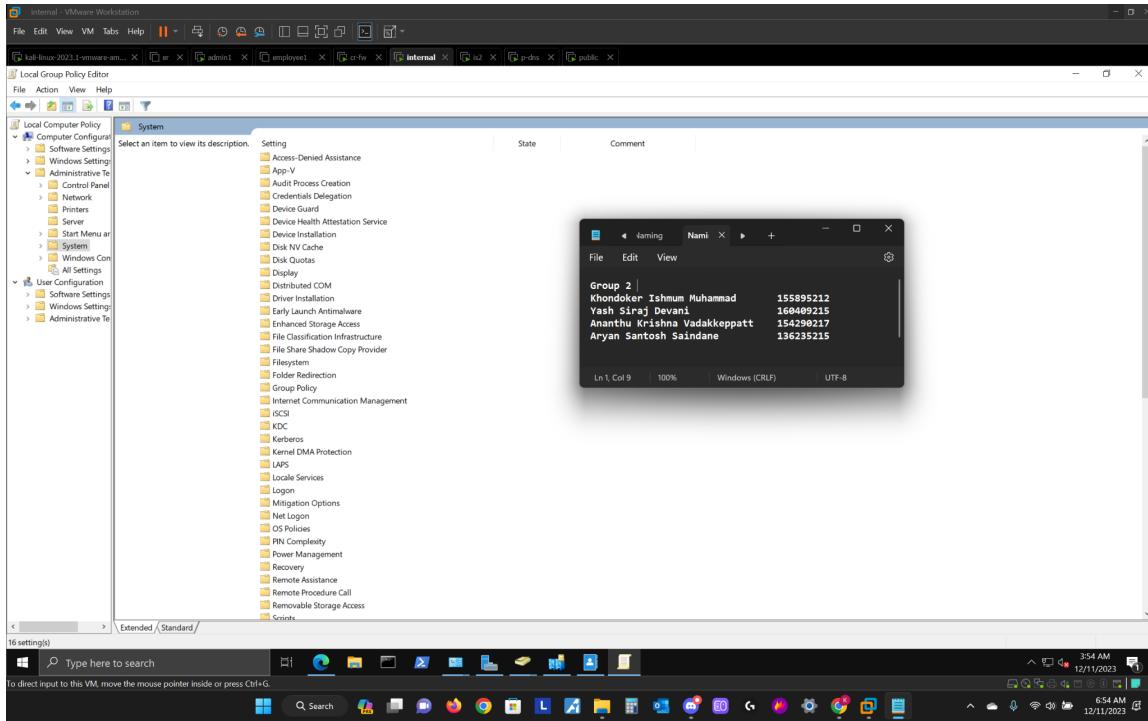
12. Incident Response Planning

- Stress the importance of creating an incident response plan to efficiently handle and mitigate the impact of phishing incidents. Incident response planning is a pivotal step in the field of cyber security. It can be used to handle and mitigate security breaches in a structured and well organized manner. The planning must utilize identifying potential threats, fast actions to come up with a plan to mitigate the threats so that the level of impact can be reduced.

13. Regular Security Assessments for Active Directory

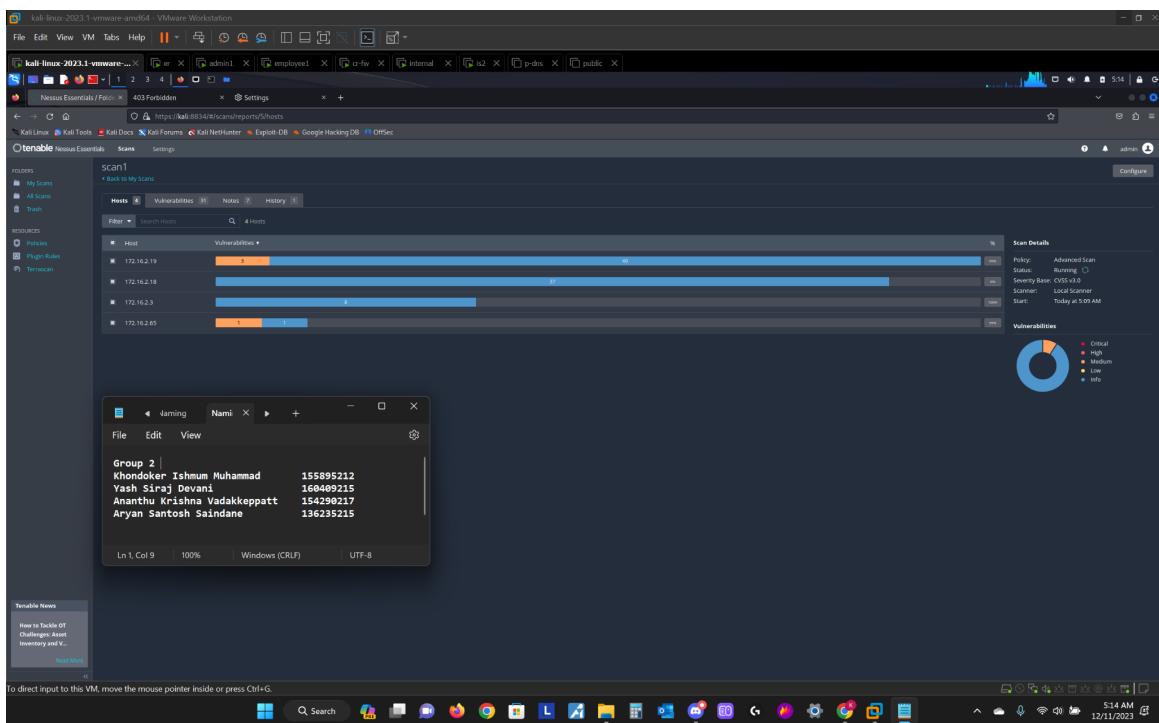
- Highlight the need for regular security assessments and penetration testing to identify and address vulnerabilities in the Active Directory environment. Also making sure to check active directory group policies.





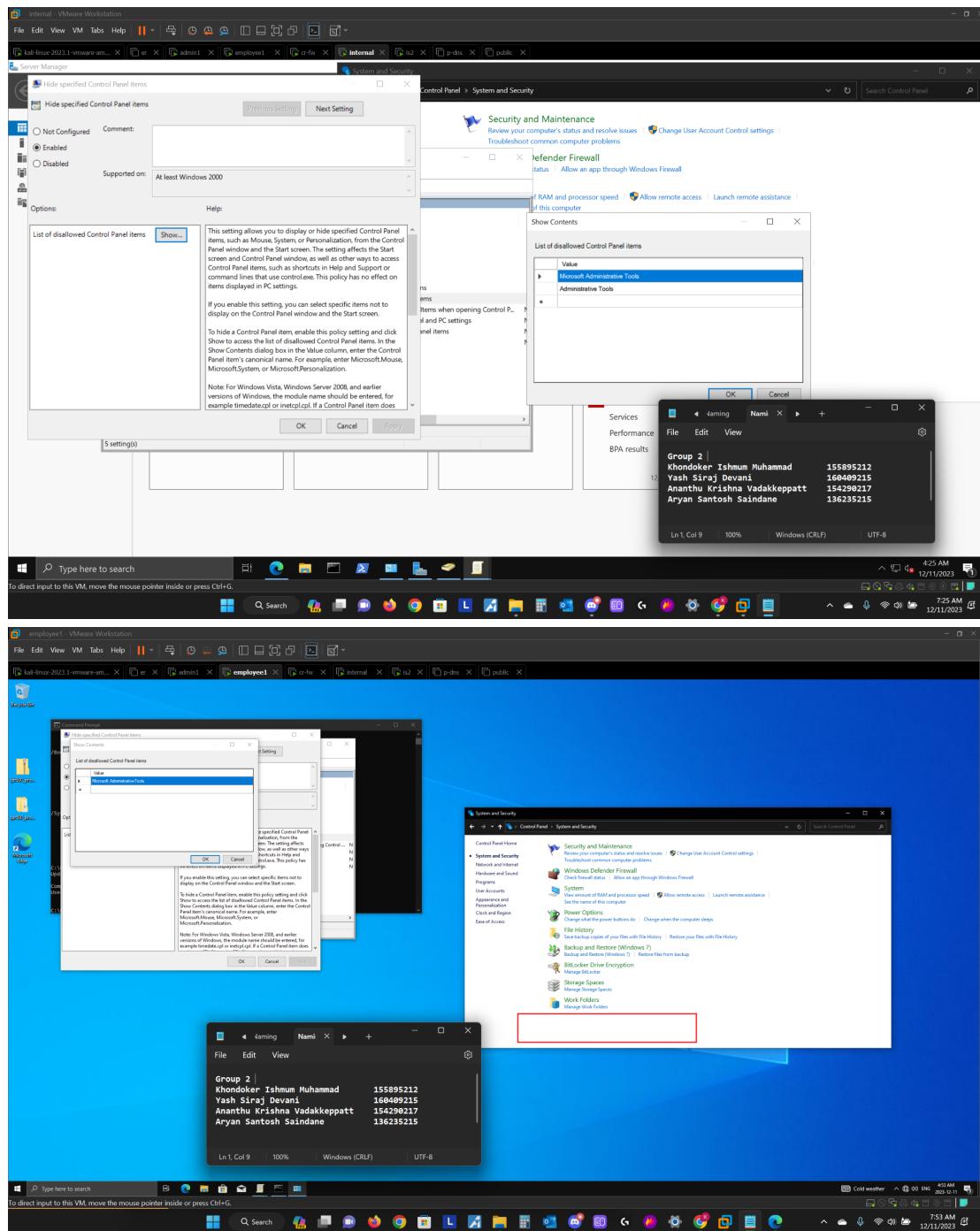
14. Lateral Movement Prevention

- Conduct regular penetration testing to identify and eliminate potential lateral movement paths. This can be done through scans to find out vulnerabilities and then seeing if those vulnerabilities can be exploited. Then after exploiting those vulnerabilities, steps should be taken to patch those vulnerabilities to mitigate their risks. By patching these vulnerabilities we can prevent malicious actors from pivoting from one device to another. This in turn can also prevent malicious actors from gaining unauthorized access to confidential data.



15. Account Access Management

- Ensuring robust access management is essential for enterprise security, incorporating measures like role-based access permissions so that users who are not authorized do not get access to unauthorized admin tools. As we can see below, administrative tools no longer appear for employee user.



16. SSL Certificates & CA For Secure HTTPS and Trust In Browser.

- Implementing SSL certificates is pivotal for enhancing security, providing encrypted communication between users' browsers and servers to prevent unauthorized

access and safeguard sensitive information during data transmission. Also utilize SSL Certificate CA and create certificate chains to ensure trust in browsers.

The screenshot displays a Linux desktop environment with multiple windows open:

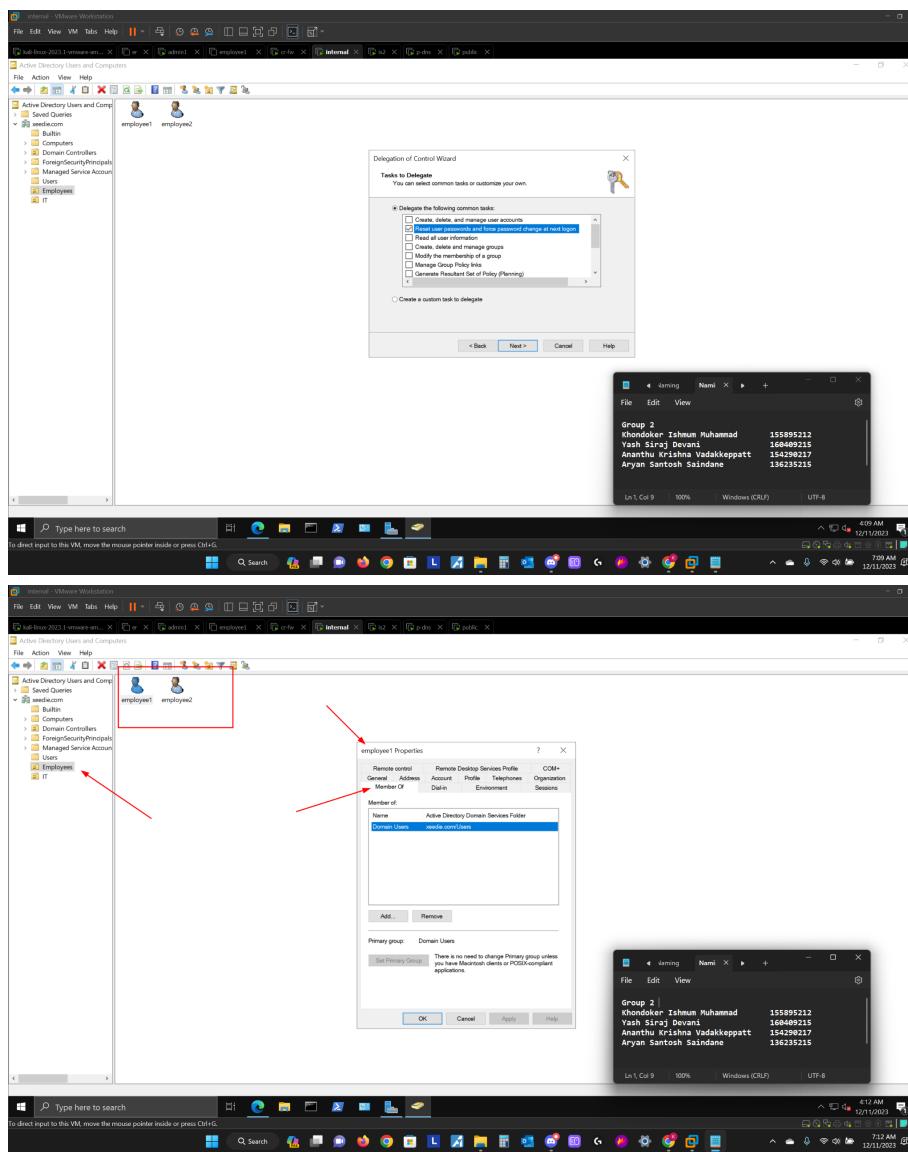
- Top Window:** A Firefox browser window showing the website <https://is2.xeedie.com/>. The address bar indicates "Connection secure". The page content includes sections for "Active Projects" and "Completed Projects".
- Middle Window:** A terminal window titled "Administrator" showing a list of names under "Group 2".
- Bottom Window:** A file manager window titled "admin1 - VMware Workstation" showing a certificate chain. It contains files like "is2.xeedie.com-chain.pem", "is2.xeedie.com.pem", and "is2.xeedie.com[1].pem".

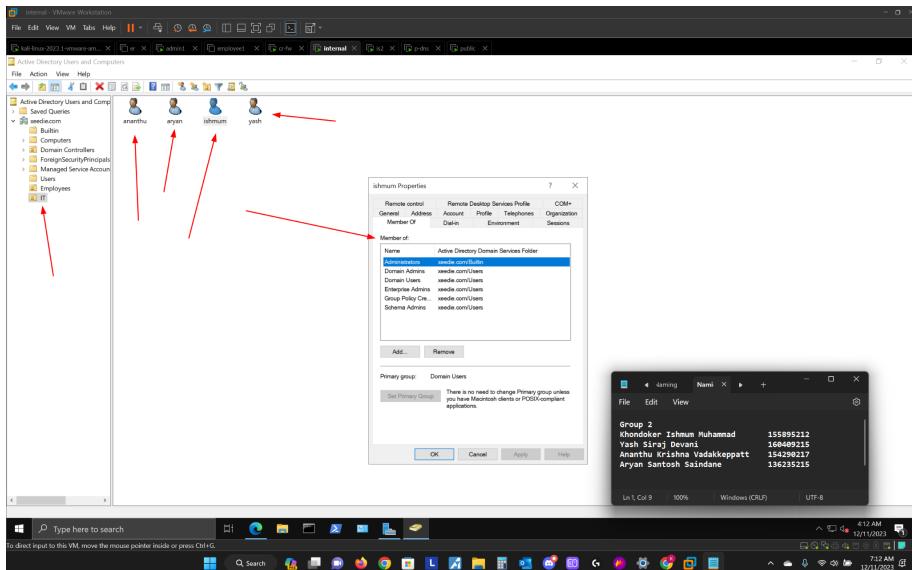
17. Host based Firewall utilization

- Using a host-based firewall to proactively block malicious traffic, ensuring the security of the network.

18. Active Directory Domain User & Groups Management

- Ensuring robust user and group management is essential for enterprise security, incorporating measures like setting specific roles for specific users and adding users in groups depending on their title is essential for a secure environment and to mitigate the risk of unauthorized access to sensitive data.





Conclusion

The security testing report for Agricore's infrastructure signifies the successful integration of security controls in alignment with CIS recommendations. Notably, access management controls, including Role-Based Access Control (RBAC) facilitated by Group Policy Objects (GPOs), were implemented to assign authorized personnel appropriate access privileges. The report emphasizes the effective deployment of audit log management controls, utilizing Snort IDS to establish robust logging mechanisms for monitoring and responding to suspicious activities. Additional measures were taken to bolster web browser security through the implementation and testing of SSL. Furthermore, a thorough evaluation of data backup and recovery solutions ensured the reliability of backup processes. In conclusion, the report affirms the establishment of a well-designed security control framework within the Agricore infrastructure, demonstrating a proactive approach to fortifying defenses against potential threats and vulnerabilities.